EUROPEAN
COMMISSION

Brussels, 7.12.2018
SWD(2018) 492 final

COMMISSION STAFF WORKING DOCUMENT

Counterfeit and Piracy Watch List

TABLE OF CONTENTS

1. INTRODUCTION

In an innovation driven global economy, infringements of intellectual property rights (IPR), in particular commercial scale counterfeiting and piracy, pose a major problem for the European Union (EU). IPR infringements cause high financial losses for European rightholders and sustainable IP-based business models. The EU has a particular interest in IPR enforcement considering that European companies are leading providers of IP-protected goods and services in third countries' markets.

A recent study[1] undertaken by the Organisation for European Cooperation and Development (OECD) and the European Union Intellectual Property Office (EUIPO) shows that international trade in counterfeit and pirated goods represents up to 2.5% of world trade, or as much as EUR 338 billion. In the EU, counterfeit and pirated goods amount to up to 5% of imports or as much as EUR 85 billion. The *quantification of intellectual property rights (IPR) infringement studies*[2] recently prepared by the European Observatory on Infringements of Intellectual Property Rights confirmed that counterfeiting and piracy cause serious sales and revenue losses for companies leading to direct and indirect jobs losses in the European Union and government revenue losses in the EU Member States.

IPR infringements must therefore be targeted as a threat to the IPR-intensive industries and to the society at large. Besides the reduction in innovation and creativity, lost sales, jobs and government revenues, IPR infringements cause significant risks to consumer health and safety and to the environment. This is particularly relevant in relation to counterfeiting. Counterfeit pharmaceutical, health and beauty products as well as tobacco and alcohol can lead to health problems. In the engineering and technology sectors, non-genuine car parts and counterfeit machinery can result in injuries and put lives in danger. Counterfeit electrical appliances and batteries, not subject to appropriate quality checks, can carry a high safety risk for the consumer.

The EUIPO-Europol *2018 Situation Report on Counterfeiting and Piracy in the European Union*[3] confirms that counterfeits almost always represent some form of risk to consumer welfare because there are invariably scant quality controls or certification protocols in place during manufacture. This affects food or pharmaceutical industries, but also has less obvious consequences in the form of the health dangers associated with substandard (flammable) clothing, dangerous toys, inferior sports shoes or sunglasses. As regards the danger to the environment, counterfeit pesticides often contain toxic substances that may contaminate soil, water and food. The Report establishes that organised criminal groups involved in IPR crime are also often engaged in other crimes, such as drug trafficking, excise fraud, human trafficking or money laundering. EU-based criminal gangs rely predominantly on manufacturers based in third countries, then organise importation, transportation, storage and distribution of the counterfeit goods within the EU. The *Internet Organised Crime Threat Assessment*[4] prepared by Europol in 2017 confirms the link between counterfeiting and piracy

[1] *Mapping the economic impact of trade in counterfeit and pirated goods* – 2016 https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Mapping_the_Economic_Impact_study/Mapping_the_Economic_Impact_en.pdf

[2] The *quantification of intellectual property rights (IPR) infringement studies* https://euipo.europa.eu/ohimportal/en/web/observatory/quantification-of-ipr-infringement

[3] *EUIPO-Europol 2018 Situation Report on Counterfeiting and Piracy in the European Union* https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union

[4] *Internet Organised Crime Threat Assessment* https://www.europol.europa.eu/activities-services/main-

and internet organised crime as another major threat to our society. The relation between counterfeiting and piracy and cybercrime is particularly clear where copyright protected content is offered and distributed through online markets that may also be used for committing cybercrimes, including distribution of malware.

A comprehensive package of measures to improve the application and enforcement of IPRs within the EU, at the EU border and globally was presented in the *Communication on A balanced IP enforcement system responding to today's societal challenges* in November 2017.[5] While a number of the actions under the framework of this Communication concern the improvement of IPR enforcement within the EU and the strengthening of customs authorities at the border, one section focuses specifically on the efforts to fight IP infringements globally. Among the specific actions in the fight against IP infringements in third countries, the Commission undertook to prepare a Watch List of the most problematic online and physical markets situated outside the EU that are reported to engage in or facilitate IPR infringements.

Against this background and in accordance with the *" Trade for all" Communication*[6] and the *Strategy for the Enforcement of Intellectual Property Rights in Third Countries*[7] the Commission services have prepared this "Counterfeit and Piracy Watch List" (the "Watch List").

The Watch List reflects the results of stakeholder consultations. It presents examples of reported marketplaces or service providers whose operators or owners are allegedly resident outside the EU and which reportedly engage in, facilitate or benefit from counterfeiting and piracy. The aim is to encourage the operators and owners as well as the responsible local enforcement authorities and governments to take the necessary actions and measures to reduce the availability of IPR infringing goods or services on these markets. The Watch List also intends to raise consumer awareness concerning the environmental, product safety and other risks of purchasing from potentially problematic marketplaces. The Watch List focuses on online marketplaces as piracy and the distribution of counterfeits increasingly take place through the internet.

The Watch List is not an exhaustive list of the reported marketplaces and service providers and does not purport to make findings of legal violations. Nor does it provide the Commission services' analysis of the state of protection and enforcement of IPR in the countries connected with the listed marketplaces and service providers. A general analysis of the protection and enforcement of IPR in third countries can be found in the Commission services' separate biennial *Report on the protection and enforcement of intellectual property rights in third countries*[8] *(Third country report*), the latest of which was published on 21 February 2018.

---

reports/internet-organised-crime-threat-assessment-iocta-2017

[5] *Communication on A balanced IP enforcement system responding to today's societal challenges* https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-707-F1-EN-MAIN-PART-1.PDF

[6] *Trade for All Communication* https://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153846.pdf

[7] *Strategy for the Enforcement of Intellectual Property Rights in Third Countries* http://trade.ec.europa.eu/doclib/docs/2014/july/tradoc_152643.pdf

[8] *Report on the protection and enforcement of intellectual property rights in third countries* http://trade.ec.europa.eu/doclib/docs/2018/march/tradoc_156634.pdf

2. METHODOLOGY

2.1. Sources

The Commission services conducted a public consultation between 8 February and 19 April 2018.[9] Its results form the basis of the Watch List.

In addition to the support of EUIPO and Europol (Intellectual Property Crime Coordinated Coalition), a number of other sources also played a role in the selection process and in defining and describing the listed marketplaces:

Information from the Commission services
- Information on IP policy received from Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs;
- Information received from EU Delegations and Offices;
- Information received from the Directorate-General for Taxation and Customs Union on customs enforcement of intellectual property rights by EU Member States[10];

EUIPO reports and studies
- Studies on the economic impact of counterfeiting and piracy[11] and on the trade routes of fake goods[12];
- Sectoral Studies[13];
- Study on Infringing Online Business Models[14];
- Study on Digital Advertising on Suspected Infringing Websites[15];

Information from the EU Member States
- Decisions of national courts;
- City of London Police IP Crime Unit's (PIPCU) Infringing Websites List[16];
- Danish list of IP infringing websites[17];
- List of the Spanish Intellectual Property Commission[18];

Other relevant sources
- Europol situation reports[19] and crime threat assessments[20];

---

[9] Please see details on the public consultation in Section 3.
[10] https://ec.europa.eu/taxation_customs/sites/taxation/files/report_on_eu_customs_enforcement_of_ipr_2017_en.pdf
[11] See *footnote 1*
[12] *Mapping the real routes of trade in fake goods* https://euipo.europa.eu/ohimportal/en/web/observatory/mapping-the-real-routes-of-trade-in-fake-goods
[13] See *footnote 2*
[14] *Study on Infringing Online Business Models* https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf
[15] *Study on Digital Advertising on Suspected Infringing Websites* https://euipo.europa.eu/ohimportal/documents/11370/80606/Digital+Advertising+on+Suspected+Infringing+Websites
[16] *City of London Police IP Crime Unit's (PIPCU) Infringing Websites List* https://www.iabuk.com/policy/infringing-website-list-iwl
[17] This list is not available publicly.
[18] List of the Spanish Intellectual Property Commission: http://www.culturaydeporte.gob.es/cultura-mecd/dms/mecd/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pirateria/2018_3Q_Report-Secc2-CPI.pdf
[19] See *footnote 3*

- Global Online Piracy study by Institute for Information Law (IViR) of the University of Amsterdam[21];
- List of IP-infringing websites by the French collecting society SACEM[22];
- Alexa[23] and SimilarWeb[24] popularity ranks;
- Google Transparency Reports[25];
- Reports by consumer alliances and brand protection companies;
- Reports and assessments made by other relevant bodies and organisations (e.g. the OECD).

2.2. Selection

All selected marketplaces are located outside the EU. Online marketplaces are considered to be located outside the EU for the purposes of this Watch List if their operator or owner is known or assumed to be resident outside the EU, irrespective of the residence of the domain name registry, the registrar, the residence of the hosting provider or the targeted country. As regards physical marketplaces, the market is considered located outside the EU if it is physically located in the territory of a third country irrespective of the citizenship or residence of its landlord. The selection of the marketplaces to be included in the Watch List was undertaken between 18 June and 20 July 2018. Consequently the information included in the report reflects the situation during this period.

The main criteria for the selection of both online and physical marketplaces to be included in the Watch List are their reported widespread global or regional popularity and high volume of sales. In order to identify websites that are popular globally or regionally, Alexa and

---

[20] See *footnote 4*

[21] *Global Online Piracy study by Institute for Information Law (IViR) of the University of Amsterdam* https://www.ivir.nl/publicaties/download/Global-Online-Piracy-Study.pdf

[22] This list is not available publicly.

[23] The EUIPO's *Study on Digital Advertising on Suspected Infringing Websites* describes that "Alexa is a web metrics company that provides data about the measure of a website's popularity compared with all of the other websites on the Internet. This data considers both the number of visitors and the number of pages viewed on each visit. Alexa collects traffic data daily from millions of users who have installed the Alexa toolbar and from direct measurements from websites that have incorporated Alexa code, and then uses a proprietary formula to create a popularity ranking for each website. A website's Alexa Rank can be interpreted as the website's position in a league table, with the most popular website given a rank of 1, the next 2 and so on through millions of websites. Alexa provides information about the ranking of websites by country and creates top 500 most popular website lists by country. Alexa also provides a global top 500 ranking representing the most popular websites in the world according to Alexa".

[24] The EUIPO's *Study on Digital Advertising on Suspected Infringing Websites* describes that "SimilarWeb uses big data technology to estimate websites' unique visitors from desktops and the origin of those visits. SimilarWeb provides information on: (1) global rank, rank of site in top country, and category rank (i.e. Rank 15 in the category of File Sharing), as well as the up or down trend in popularity; (2) total visits each month for the past 6 months; (3) traffic sources (35% direct, 33% referrals, 14% search, 7% social); (4) top 5 referring sites and top 5 destination sites; (5) leading organic keywords that users searched that led them to the site; (6) percentage of social networks sending traffic to the site; (7) top ad networks and leading publishers referring advertising traffic to the website; (8) audience interests including a short list of websites frequently visited by the website's users; (9) similar sites and (10) related mobile apps".

[25] The EUIPO's *Study on Digital Advertising on Suspected Infringing Websites* describes that "Google regularly receives requests from copyright owners and their agents and organisations that represent them to remove search results that link to content or goods allegedly infringing IP rights. Google makes available online a report that specifies the number of requests it receives to remove search results, and indexes the results by domains, copyright holders, reporting organisations and requests. The Google Transparency Report indicates the volume of infringement takedown requests sent by parties to Google for search takedowns in relation to websites that may infringe copyright. The listed copyright related websites were cross-checked with the Google Transparency Report for specific organisations to identify websites with the highest number of infringing link notices sent to Google by key IP rights holders and other IP content protection associations".

SimilarWeb web popularity ranks and Google's Transparency Reports for copyright related websites were used. Both the marketplaces that are visited from the EU and those that are visited only from third countries but harm EU rightholders and trade with these countries were taken into account.

All online marketplaces included in the Watch List were reviewed and assessed for suspected copyright infringing content or suspected counterfeit goods. To search for suspected pirated or counterfeit goods or content, popular European content titles or brands were used.

Measures taken by online marketplaces with regard to the principles recommended in the Commission's *Recommendation on measures to effectively tackle illegal content online*[26] (e.g. the need for a clear notification procedure, transparent policy for the removal or disabling access to the content, regular activity reports, the use of automated means for the detection of illegal content, cooperation with rightholders and enforcement authorities) were reported by stakeholders and also taken into account in the preparation of the Watch List.

2.3. Structure

Marketplaces were grouped on the basis of the business model and type of technology they use to distribute goods and services. Service providers facilitating IPR infringements were categorised on the basis of the nature of service they provide to facilitate the distribution of goods and services (i.e. hosting provider, advertising agency, domain name registrar). The chapters and sections in the Watch List reflect the different marketplace and service provider types.

The chapter on e-commerce platforms reflects the fact that they – differently from other marketplaces and service providers - facilitate the sales of physical products in an online environment (be it business-to-business, business-to-consumer or consumer-to-consumer sales).

A separate chapter is dedicated specifically to illicit online pharmacies. These platforms offer for sale all kinds of medicines and arrange their delivery to consumers. Due to the major health risks to EU consumers involved, the marketplaces that are reportedly often visited by EU consumers were identified. Illicit online pharmacies operate in clusters and hence the aim was identifying these clusters and the domain name registrars[27] facilitating their operation.

Despite the growing significance of online trade, the sales of counterfeit goods in physical marketplaces continue to be rife around the world. A chapter is therefore dedicated to the most prominent physical marketplaces.

[26] *Commission Recommendation on measures to effectively tackle illegal content online* https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[27] Domain name registrars are accredited organisations that sell domain names to the public.

3. RESULTS OF THE PUBLIC CONSULTATION

More than 70 responses were received through the public consultation[28], covering both online and physical marketplaces located in more than 20 countries. The majority of the respondents were businesses, associations representing rightholders and associations fighting against IP infringements. Individuals, law firms, chambers of commerce and brand protection companies also sent their contributions. Information regarding the respondents and their contribution is published along with the Watch List, unless otherwise requested by the respondent.

On online marketplaces, more responses were received from the creative industries than from brand owners. The creative industries and associations fighting piracy focused almost entirely on websites and have not requested to list physical marketplaces. Cyberlockers, peer-to-peer networks and BitTorrent indexing websites received the most reports, followed by stream-ripping and linking sites as well as unlicensed pay-per-download sites. The creative industries expressed grave concerns about the role of certain hosting providers, registries, registrars and ad-networks in facilitating online piracy.

Broadcasting organisations and their trade associations reported mainly streaming and linking websites which make available allegedly pirated audiovisual content (i.e. films, TV programmes and sport events). A particular concern for this industry is the illegal streaming of live sport events. This constitutes a particular challenge for the enforcement authorities as such illegal streaming sites should be blocked at the time of the sport event. Besides, broadcasting organisations raised concerns about some e-commerce platforms which offer for sale allegedly illegal IPTV set-top-boxes and IPTV subscriptions.

Brand owners (sport, automotive, luxury, fashion, footwear, electronics, cosmetics), brand associations, chambers of commerce, brand protection companies and associations fighting against counterfeiting, reported both physical marketplaces and e-commerce platforms. The majority of the e-commerce platforms reportedly operate from China or South East Asian countries but e-commerce platforms from other regions were also reported. Stakeholders also reported a high number of offers of counterfeit goods on social media.

Some e-commerce platforms provided detailed information on the measures they take to reduce the availability of counterfeit offers on their platforms, relying in part on the key performance indicators introduced by the *Memorandum of Understanding on the sale of counterfeit goods via the internet*[29]. The MoU on the sale of counterfeit goods via the internet is a voluntary agreement facilitated by the European Commission to prevent offers of counterfeit goods from appearing in online marketplaces.

European pharmaceutical companies and industry associations provided detailed information on the ecosystem of illicit online pharmacies and reported several online marketplaces offering for sale different kinds of medicines. In addition, European pharmaceutical companies, industry associations and alliances fighting against illicit online pharmacies reported that some domain name registrars also facilitate the business of illicit online pharmacies by not having or not enforcing policies against counterfeit medicines and thus

[28] http://trade.ec.europa.eu/doclib/docs/2018/january/tradoc_156552.pdf

[29] The MoU is limited to each signatory to the extent that it provides services in the Member States of the European Union / European Economic Area. *Memorandum of Understanding on the sale of counterfeit goods via the internet* https://ec.europa.eu/growth/industry/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en

represent a safe harbour for illicit online pharmacies.

With regards to physical marketplaces, most of the reports were received from brand owners (sport, automotive, luxury, fashion, footwear, electronics, cosmetics), chambers of commerce and associations fighting against counterfeiting for markets located in China and India, followed by markets situated in South East Asian countries. According to stakeholders, counterfeiters use free trade zones, including those located in the United Arab Emirates, to manufacture, store and tranship allegedly counterfeit goods to various destinations, including the European Union, camouflaging the original point of production and/or departure[30] [31].

4. NEXT STEPS

The Commission services will use the Watch List to continue the cooperation with EU's trading partners in the framework of IPR Dialogues and working groups. The IPR Dialogues and working groups enable the exchange of information on multilateral and bilateral IPR enforcement-related issues, including on national IPR enforcement legislation and practices, in order to identify shortcomings and make proposals for improvement.[32] The Watch List will also be used in the framework of the four-year-long technical cooperation programmes IP Key China[33], Southeast Asia[34] and Latin America[35] which were launched in 2017. The Watch List will be updated regularly by the Commission services. The Commission services will also monitor the measures and actions taken by the local authorities in relation to the listed marketplaces as well as the measures and actions taken by the operators and marketplace owners to curb IPR infringements.

5. ONLINE MARKETPLACES OFFERING COPYRIGHT-PROTECTED CONTENT

The ways in which consumers enjoy content such as music, films, books and video games have changed drastically over the past 15 years. Copyright-protected content used to be acquired mostly in the form of physical carriers (e.g., CDs, DVDs, books), whereas nowadays the Internet is becoming the main mean of content distribution. Piracy followed the same pattern and shifted from physical to online piracy. This chapter is dedicated to online marketplaces that offer content protected by copyright and/or related rights and service providers that facilitate access to this content. The listed marketplaces and service providers are grouped according to the business model and technology they employ. For the preparation of this section measures taken by online marketplaces with regard to the principles recommended in the Commission's *Recommendation on measures to effectively tackle illegal content online*[36] published on 1 March 2018 were also taken into account.

[30] *Trade in counterfeit goods and free trade zones* http://www.oecd.org/publications/trade-in-counterfeit-goods-and-free-trade-zones-9789264289550-en.htm
[31] See *footnote 1*
[32] In this context, the Commission regularly meets with China, Taiwan and Hong Kong, Korea, Brazil, Chile, Thailand, Turkey and Ukraine.
[33] https://ipkey.eu/en/china
[34] https://ipkey.eu/en/south-east-asia
[35] https://ipkey.eu/en/latin-america
[36] See *footnote 26*

a) Cyberlockers

A "cyberlocker" is a type of cloud storage and cloud sharing service which enables users to upload, store and share content in centralised online servers. The content is managed by the owner of the website. Both legal and illegal content can be stored and shared in cyberlockers, but a clear difference can be drawn between the business models of rogue cyberlockers that are engaged in content theft and legitimate cloud storage services.

Rogue cyberlockers incentivise their users to upload popular files to their servers. These uploaded files are then downloaded or streamed by other users. Cyberlockers generate a unique URL link (or sometimes several URL links) to access the uploaded file enabling clients to download or stream the content. The URL link is usually promoted across the Internet by different means, like social media platforms, blogs, emails, mobile applications or linking in other websites. In this way, according to the film, TV, music, software and book publishing industry, cyberlockers facilitate widespread access to high volume of infringing content uploaded anonymously onto their servers.

Cyberlockers usually earn their revenue from online advertising or the sale of premium accounts, which offer users different kinds of benefits (such as increased download speeds). These premium accounts are popular among those users who download large, mainly audiovisual files. According to *NetNames's and Digital Citizens Alliance's Behind the Cyberlocker Door report*[37], 70,6% of the cyberlockers' revenue comes from premium accounts and 29,4% from advertising. The rewards offered to users by cyberlockers depend on the size of the downloaded file, the location of the downloader and also on the number of times the content was downloaded or streamed.

Stakeholders reported that cyberlockers are harmful, also because they often make available pre-release content (content which has not yet been commercially released), which has negative effects on the revenue of creative industries.

Another difference between legitimate cloud storage services and rogue cyberlockers is that cyberlockers usually mask the identity of their operators via domain privacy services and via offshore companies, which makes it hard for enforcement authorities to link these sites to any natural person. A further complication for the enforcement authorities is that cyberlockers often generate several unique links to the same file and use proxy servers to hide the locations of the hosted content. It was also found that more than half of all cyberlockers were responsible for malware infections on user computers and that users may be subjected to identity theft and viruses when using them[38].

The music and film industry reported that the listed cyberlockers had received notices to take down content and that many were also sent cease and desist letters, but they had not reacted and had not removed the content.

***Rapidgator.net* (*rg.to*)**

Rapidgator.net is a direct download cyberlocker site, hosted in Switzerland but allegedly

[37] *NetNames's and Digital Citizens Alliance's Behind the Cyberlocker Door report* https://media.gractions.com/314a5a5a9abbbbc5e3bd824cf47c46ef4b9d3a76/7843c97d-fd81-4597-a5d9-b1f5866b0833.pdf

[38] *See footnote 37*

operated from Russia, which offers allegedly infringing music, films, TV programmes, books and video games mainly to users outside the EU.

Beyond the revenue generated by online advertising, *Rapidgator.net* offers monetary rewards and affiliate schemes[39], which encourage uploaders to make available popular content such as films, music and television programmes. Unlimited download speed and parallel downloads are available to premium users, as well as instant downloads without any wait restriction. Users who upload files are rewarded for every 1,000 downloads and for the premium membership, the user making the referral[40] is paid a certain share of the sale. Files above a certain size cannot be downloaded, unless the user has a premium membership. According to *NetNames's and Digital Citizens Alliance's Behind the Cyberlocker Door report*[41], *Rapidgator.net* generated approximately $3,7 million in annual revenue.

The total number of visits of *rapidgrator.net* between April 2017 and March 2018 was around 635,7 million. The average website rank worldwide was 1184 in this period. 34% of the visits came from the EU, 66% from non-EU countries. The service is most popular in Japan, with the highest combination of visitors and page views for the site.

***Uploaded.net* (*ul.to*, *uploaded.to*)**

Uploaded.net is a direct download cyberlocker, hosted in Germany and allegedly operated from Switzerland, which offers access to a broad range of reportedly infringing content such as books, films, TV programmes and music, including pre-releases.

It has a reward scheme to generate income and to incentivise the sharing of content. The site rewards users for large files like films and TV programmes and for high numbers of download. Registration options for users include free or premium accounts. Premium account fees depend on the desired duration of the account (from 48 hours to 2 years). Premium account holders have access to full speed download, unlimited storage for uploaded files, parallel and ad-free downloads without restrictions and earning options. In addition, *Uploaded.net* also provides direct payments to users who upload files which are downloaded more than 1,000 times. The "download rewards" rise if downloads come from countries like the UK, France, Belgium, Spain or Germany.

The total number of visits of *Uploaded.net* between April 2017 and March 2018 was around 856 million. The average website rank worldwide was 1140 in this period. 39% of the visits came from the EU, 61% from non-EU countries. Courts in Germany[42], India[43] and Italy[44] have issued blocking orders against the site.

[39] By using an affiliate scheme, other websites (the affiliates) have a link to the cyberlocker website and then if a visitor follows that link and downloads something from the cyberlocker, a small commission on that sale is also paid to the affiliate.
[40] Referral is a recommendation from one website to another.
[41] *See footnote* 37
[42] District Court of Munich I, 21 O 6197/14, 10 August 2016; link (unofficial source): https://www.jurion.de/urteile/lg-muenchen_i/2016-08-10/21-o-6197_14/
[43] Precautionary blocking injunction of the Judge for the Preliminary Investigation (Giudice per le Indagini Preliminari - GIP) of Rome, 27 February 2013.
[44] High Court of Delhi, CS(OS) 1860/2014, 23 June 2014, I.A. No. 11577/2014; link (official source): http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=119642&yr=2014

***Openload*[45]**

Openload is one of the most popular streaming cyberlockers worldwide reportedly offering unauthorised copies of films, TV shows, books and music. The hosting provider of the website is not revealed by a service provider registered in the US. The website incentivises users to upload large, popular files by paying a fixed reward per 10,000 downloads or streams. The total number of visits of *Openload.co* between April 2017 and March 2018 was around 3,2 billion. The average rank worldwide was 267. 37% of the visits came from the EU, 63% from non-EU countries.

4shared.com

4shared.com is one of the most popular direct download cyberlockers worldwide and reportedly offers unauthorised copies of films, TV shows, books and music. It is hosted in the US and the residence of its operator is assumed to be outside the EU. According to a report prepared by NetNames and Digital Citizens Alliance: *Behind the Cyberlocker Door*[46]*, 4Shared.com* has the highest unique visitors among the direct download cyberlocker sites globally and makes the highest profit.

4Shared.com offers a premium account and a reward scheme for users who upload popular content. *4Shared.com* mobile apps reportedly enable users to stream infringing content to mobile devices. The site has income from advertising and from its basic and premium accounts. The total number of visits of *4shared.com* between April 2017 and March 2018 was around 721 million. The average rank worldwide was 639 in this period. 10% of the visits came from the EU, 90% from non-EU countries. The Korean Communications Standard Commission issued a blocking order[47] in respect of this cyberlocker in October 2014.

Sci-hub.tw/#about[48] and ***Library Genesis Group***[49]

Sci-hub.tw/#about is one of the most problematic online actors for book and scholarly publishers according to the European publishing industry. Sci-hub.tw/#about and its operator are hosted in Russia. The site reportedly provides unauthorised access to around 55-60 million journal articles, academic papers and books. Sci-hub.tw/#about allegedly gains unauthorised access to a publishers' journal database by using compromised user credentials obtained via phishing scams. Once it gains access to the journal database, it downloads articles, stores them on its own servers and makes them available to the requesting users, while continuing to cross-post these articles to Sci-hub.tw/#about and its related sites. Though the site operator claims to have no knowledge of illegal tactics used to trick legitimate subscribers into disclosing their personal credentials, compromised universities and other institutions have reported instances to the European book publishing industry whereby their students and academic personnel have been subject to phishing scams[50]. The average rank worldwide was 247,601 between April 2017 and March 2018.

---

[45] *oload.tv, openload.co, openload.io, oload.stream, openload.link, openloadmovies.net*
[46] See *footnote 37*
[47] 19th standing committee of the Korean Communication Standards Commission (KCSC), decision of 14 October 2014; link http://transparency.kr/case/258
[48] also previously *sci-hub.cc*; *sci-hub.ac*; *sci-hub.bz*
[49] *Libgen.io* and its mirror sites
[50] For instance, emails claiming that a student's library access is due to expire and the individual is required to "update" his/her login credentials through a conveniently provided link (that harvests the individual's personal, private information).

The United States' courts ordered the domain registries to suspend *Sci-hub.io'*s and its mirror sites domain names in 2015. Afterwards, the United States' district court in the Southern District of New York[51] ruled that the site is liable for wilful infringement of copyrights.

Libgen.io is reportedly the most popular website in the so-called Library Genesis Group. It is a cyberlocker site hosted in both Russia and the Netherlands and operated from Russia, which allegedly operates a repository of pirated publications, including books, scientific, technical and medical journal articles as well as scholarly materials. It has a number of mirror sites making the same content available: *libgen.pw*, *lib.rus.ec*, *bookre.org*, *booksc.org*, *book4you.org*, *bookfi.net* and *b-ok.org*. The average rank worldwide was 2,320. The website is blocked by the Italian Regulatory Authority for Communications[52]. The site remains subject of a blocking order in the UK[53].

The vast majority of the scientific, technical and medical journal articles on *Libgen.io* were reportedly obtained via *Sci-hub.org*. Advertising is a source of income for the site and it also invites users to make donations.

Bookfi.net, another important website of the Library Genesis Group makes available more than 2.2 million allegedly unauthorised copies of books. It is operated allegedly from Russia or Ukraine. Advertising is a source of income for the site which also invites users to make donations. The average rank worldwide was 27,194 between April 2017 and March 2018. The site remains subject to a blocking order in the UK[54].

B-ok.org is another relevant website in the Library Genesis Group. It offers access via download to more than 3 million books (reportedly the biggest collection of e-books) and more than 52 million articles, largely illegally, according to the European book publishing industry. The average rank worldwide was 17,465 between April 2017 and March 2018. The site is operated allegedly from China. Users who register with email and password are able to increase their daily downloads limit, use an e-book converter, submit book reviews and use other features.

b) <u>Stream-ripping websites</u>

Stream-ripping services are websites, software and apps that enable users to convert and to download audio and audiovisual content from online streaming platforms. Stream-ripping services enable users to copy the URL of a content taken from a streaming platform and paste it into a search box on the stream-ripping site. When the user clicks on the download button, the stream-ripping site converts the content and creates a media file usually in mp3 or mp4 format with certain metadata added to the file (such as the title of the content or name of the author). These services usually circumvent the technological protection measures which are applied by the streaming platforms.

---

[51] Southern New York District Court, 15 civ. 4282 (RWS), 28 October 2015; link (unofficial source): https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2015cv04282/442951/53/

[52] Italian Regulatory Authority for Communications Decision 179/18/CSP; link (official source): https://www.agcom.it/documents/10179/11173566/Delibera+179-18-CSP/635047ae-0d9a-4d7b-8de9-47c5ae235f3e?version=1.0

[53] https://www.footanstey.com/bulletins/2835-high-court-ruling-blocking-order-imposed-on-isps-to-tackle-ebook-piracy

[54] https://www.footanstey.com/bulletins/2835-high-court-ruling-blocking-order-imposed-on-isps-to-tackle-ebook-piracy

Stream-ripping services often provide a search function on their platform (so that the user does not need to search for a link on other platforms) while stream-ripping plug-ins usually offer a specific download button placed on the streaming platform, making the ripping of the content even easier for the users.

Advertising is the main revenue source of stream-rippers, with many disseminating malware and other unwanted programme advertising[55]. According to stakeholders, stream-rippers are causing significant losses for the music, film and television industry by having a negative impact on income from legal streaming services and sales from the legal download services. The users of stream-ripping services can download protected content free-of-charge, which reduces any further need to stream content from legal services. According to the music and film industry, stream-ripping is currently the most prominent form of piracy globally.

H2converter.com

H2converter.com enables users to convert and download content from audio and audiovisual streaming platforms. According to the music industry, this is one of the most popular stream-ripping services worldwide. It is hosted in the US with an operator allegedly resident in Vietnam. The site uses domain privacy services in order to mask the domain registrar's true identity. The total number of visits of *H2converter.com* between April 2017 and March 2018 was around 312 million. The average rank worldwide was 17,290. 18% of the visits came from the EU, 82% from non-EU countries.

Downvids.net

Downvids.net allegedly enables users to convert and download content from audio and audiovisual streaming platforms. According to the music industry, this is one of the most popular stream-ripping services globally. The site is hosted in France and the residence of its operator is assumed to be outside of the EU. *Downvids.net* had global traffic of around 107 million visits between the start of April 2017 and the end of March 2018. The average rank worldwide was 26,275 between April 2017 and March 2018.

c) <u>Linking or referrer websites</u>

Linking or referrer sites aggregate, categorise, organise and index links to media content that is stored on hosting websites, cyberlockers or other kinds of sites allegedly containing pirated content. They often categorise links by content type and offer search tools[56]. Linking or referrer sites do not host the content themselves but link the users to third party sites, thereby reducing these sites' maintenance costs.

The content in linking or referrer sites is organised by title, album, genre and season. The users are provided with detailed information on the content. The users can choose to download or stream a film file or a music track or album by clicking on the download or stream button and then being redirected to another site, from where the download or

[55] *Identification and Analysis of Malware on Selected Suspected Copyright-Infringing Websites* https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2018_Malware_Study/2018_Malware_Study_en.pdf

[56] See *footnote 15*

streaming starts automatically.

Streaming linking sites often also embed video players from other sites, making the user's experience smoother in accessing the content. To avoid that takedowns on third-party sites harm their business, some linking or referrer sites also host the content. The listed linking or referrer sites pursue financial gains through income from advertising and referrals.

The music and film industries are particularly concerned, since, allegedly, linking sites often make available pre-release content. The music and film industry reported that the listed marketplaces received notices to take down content and many were also sent cease and desist letters, but they have reportedly not reacted and have not removed the content upon request.

Fullhdfilmizlesene.org

Fullhdfilmizlesene.org is one of the most popular linking websites, which aggregates, categorises, organises and indexes links to allegedly unauthorised copies of films. The website provides links to content from several cyberlockers and is regularly updated with new releases. Currently hosted in Turkey, *Fullhdfilmizlesene.org* is using a domain privacy and proxy service which hides the identity and residence of the operator. The linked content is stored on third party websites and *Fullhdfilmizlesene.org* streams it without requiring users to register. The website is categorised by genre, new films, most recommended films and most viewed films. The total number of visits of *Fullhdfilmizlesene.org* was around 450,9 million between the start of April 2017 and the end of March 2018. The average rank worldwide was 1,313 during this period.

Seasonvar.ru

Seasonvar.ru is a streaming website which allows users to access content for free. The website claims to have 10,901 accessible files. The website is currently hosted in Russia and the residence of the operator is assumed to be outside the EU. A premium subscription is available for a low price and allows users to download audiovisual content to computers or mobile phones in high definition without any advertising interruptions. The total number of visits of *seasonvar.ru* was around 1,1 billion between the start of April 2017 and the end of March 2018. The average rank of the site worldwide was 418 during this period.

Dwatchseries.to

Previously *xwatchseries.to* and *ewatchseries.to* (and several others), *Dwatchseries.to* (redirect to *swatchseries.to*) appears to be one of the most popular linking or referrer sites in the world. The site is currently hosted in Switzerland and uses masking services, which hides the IP location of the website. The total number of visits of *Dwatchseries.to* was around 156,4 million between the start of April 2017 and the end of March 2018. The average rank of the site worldwide was 920 during this period. Derived and mirror sites of the website have been subject to blocking orders in Australia[57], Denmark[58], Ireland[59], Norway[60] and the United

[57] Federal Court of Australia, NSD 663 of 2017, 1 September 2017; link (official source): http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca1041
[58] District Court Frederiksberg, BS FOR-563/2016, 25 August 2016.
[59] High Court Dublin, 2017 No 913 P (2017 No 24 COM), 3 April 2017.
[60] District Court Oslo, Case No 16-072899TVI-OTIR/08, 22 June 2016.

Kingdom[61].

1channel.ch

1channel.ch (previously *Primewire.ag*) is one of the most visited linking or referrer sites globally offering links to allegedly illicit copies of blockbuster films and television programmes. The site claims to link to more than 76,781 free copies of films. Over the years, stakeholders report that the site has employed numerous tactics attempting to fend off enforcement measures and stay online, including hosting through a rotating inventory of thirty or more domains and a variety of hosting locations. The site also uses masking services which hide the IP location of the website. Currently using hosting facilities in Switzerland, *1channel.ch* is masked behind a reverse proxy service that curbs enforcement authorities' ability to identify its precise host. The average rank of the site worldwide was 1,238, with more than 531,8 million visits. *Primewire.ag* has been the subject of blocking orders in Australia[62], Belgium[63], Denmark[64], Ireland[65], Norway[66], Portugal[67] and the United Kingdom[68].

Rnbxclusive.review[69]

Rnbxclusive.review (and its variant sites, redirects to *rnbxclusive1.com*) is a website aggregating and indexing hyperlinks to allegedly unauthorised copies of copyright-protected content, mainly music, including also pre-releases. The hosting provider of these linking or referrer sites is not revealed by a service provider registered in the United States. The operator of the site is allegedly resident in Ukraine. *Rnbxclusive.review* had global traffic of approximately 200,000 visits between the beginning of April 2017 and the end of March 2018, however, the site has been domain hopping[70] (*rnbxclusive.top, rnbxclusive.stream, rnbxclusive.pw, rnbxclusive.me* and others) and each of these domains has had between 1 million to 2,3 million visits before the site hopped onto a new domain name extension, with the *.review* being the latest one – hence the lower traffic data so far. *Rnbxclusive* generates income from advertising. The average rank worldwide is not indicated due to the domain hopping. 27-36% of the visits on these sites came from the EU, 64-73% from non-EU countries.

[61] London High Court of Justice, HC14E02926, 14 November 2014.
[62] Federal Court of Australia, No. NSD 269 of 2017, 18 August 2017; link (official source): http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca0965
[63] Francophone Commercial Tribunal of Brussels (Tribunal de Commerce francophone de Bruxelles), R. G. : A/18/00217.
[64] Copenhagen City Court, Case No BS 21C-3723/2013, 8 October 2013.
[65] High Commercial Court Ireland, 2017 No 913 P 2017 No 24 COM, 3 April 2017.
[66] District Court Oslo, Case No 15-067093TV1-OTIR/05, 1 January 2015.
[67] General Inspection of Cultural Activities (Inspeção-Geral das Atividades Culturais – Gabinete da Direção), 1101/IG/2015.
[68] London Court of Justice, Claim No HC13B03859, 25 October 2013.
[69] *rnbxclusive.stream, rnbxclusive.top, rnbxclusive.pw, rnbxclusive.me, rnbxclusive.win, rnbxclusive.bid*
[70] After having received many notices from rightholders about a domain name used by a pirate site, the site is downranked in search results. To stay constantly high in search results, pirate sites tend to regularly switch domain names.

d) Peer-to-peer and BitTorrent indexing websites

As described by the EUIPO's Study on *Digital Advertising on Suspected Infringing Websites*[71] peer-to-peer and BitTorrent indexing websites use the peer-to-peer file distribution technology to permit users to share content. The websites act as aggregators of peer-to-peer links, which users can search for and access via the website. When a user clicks on a link, the peer-to-peer technology allows the user to download media files stored on other users' computers across the peer-to-peer network. A user in a peer-to-peer network downloads files from other users' private storage place and makes his files available for upload to the peer-to-peer network. Users offering a file are known as "seeders" and they share these files with other users known as "peers".

The users first need to download a BitTorrent client[72] in order to download a file in the BitTorrent system. Once the BitTorrent client is downloaded, users need to locate the content they want to download, click on the torrent file or the magnet link associated to the file in question. By doing this, the BitTorrent client starts receiving pieces of the file from the seeders. Once the BitTorrent client has received all the pieces of the file, it reassembles them into the completed file and saves the file on the computer of the person who initiated the download.

Indexing services usually generate income from advertisements and donations from users. BitTorrent indexing sites often register multiple domain names in order to prevent their business being damaged if one of their domain names is seized or blocked by the enforcement authorities.

ThePirateBay.org

Available in 35 languages, *ThePirateBay.org* is allegedly one of the largest BitTorrent websites globally. The website facilitates sharing all kinds of content (including films, music, TV programmes, software, videogames and books) in its peer-to-peer network.

Although copyright holders have successfully taken action against the operators of BitTorrent websites in a number of jurisdictions throughout the world and the website was closed down for a while, it reappeared and continues to be active. It released the Pirate Browser, a self-contained portable web browser with pre-set bookmarks to BitTorrent websites hosted on the TOR network[73]. The website has been reported to have multiple alternative domains hosted in various countries around the world over the years. The total number of visits of the site between April 2017 and March 2018 was around 3,1 billion. The average rank worldwide was 103 during this period.

In December 2017 the Swedish Supreme Court confirmed that domains can be seized under Swedish law, upholding the Court of Appeals' decision to seize *piratebay.se* and *thepiratebay.se* from one of the original founders. The *Pirate Bay* is blocked in Australia[74],

[71] See *footnote 15*
[72] Software that helps users to find the torrents they want, and download them quickly and safely.
[73] TOR is free software, which enables anonymous communication. It conceals a user's location and usage from anyone conducting network surveillance or traffic analysis.
[74] Federal Court of Australia, No. NSD 239 and 241 of 2016, 15 December 2016, link (official source): http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2016/2016fca1503; and Federal Court of Australia, No. NSD 269 of 2017, 18 August 2017, link (official source): http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca0965

Austria[75], Belgium[76], Denmark[77], Finland[78], France[79], Iceland[80], Ireland[81], Italy[82], Malaysia[83], Netherlands[84], Norway[85], Portugal[86], Spain[87], Sweden[88] and the United Kingdom[89].

Rarbg.to

Rarbg.to is reported to be a popular BitTorrent website hosted in Bosnia and Herzegovina providing access to a range of content, including films, TV programmes, software, videogames and music. The files are organised and displayed in content categories.

Rarbg.to is one of the BitTorrent indexing websites responding to take down notices, but the main problem with the use of take down notices on *Rarbg.to* is that the same infringing

[75] Supreme Court of Austria, No. 4 Ob 121/17y, 24 October 2017, link (official source): https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=df3a2cab-8dd1-4ce4-8795-9cdfffc0e919&Position=1&Abfrage=Justiz&Gericht=&Rechtssatznummer=&Rechtssatz=&Fundstelle=&AenderungenSeit=Undefined&SucheNachRechtssatz=False&SucheNachText=True&GZ=4Ob121%2f17y&VonDatum=&BisDatum=09.11.2017&Norm=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=JJT_20171024_OGH0002_0040OB00121_17Y0000_000

[76] Court of Appeal of Antwerpen, Section 1, No. 3399 Rep. 2011/8314, 26 September 2011; link (unofficial source): https://nurpa.be/files/20111004_BAF-Belgacom-Telenet-DNS-blocking.pdf

[77] Bailiff's Court of Frederiksberg of Copenhagen, IFPI Danmark v DMT2 A/S, No. 14324/2007, 29 October 2008; link (unofficial source): https://www.computerworld.dk/art/44279/the-court-order-to-shut-off-access-to-the-pirate-bay, confirmed in appeal by the High Court of Eastern Denmark, Sonofon A/S v IFPI, Case No. B-530-08, 26 November 2008, link (unofficial source): http://www.computerworld.dk/modules/davinci/getfile.php?id=26993&attachment, and confirmed by the Danish Supreme Court, Telenor v IFPI, No. 159/2009, 27 May 2010 link (official source): http://www.hoejesteret.dk/hoejesteret/nyheder/Afgorelser/Documents/153-2009.pdf.

[78] District Court of Helsinki, Case No. H 11/20937, 26 October 2011.

[79] Court of Appeal of Paris, Case No. 15/02735, 18 October 2016.

[80] District Court of Reykjavik, Case No. K-8/2013, 14 October 2014; link (official source): https://www.heradsdomstolar.is/default.aspx?pageid=347c3bb1-8926-11e5-80c6-005056bc6a40&id=7c92472b-9a7f-4566-bb34-722bb7f54cb3 and District Court of Reykjavik, Case No. K-9/2013, 14 October 2014; link (official source): https://www.heradsdomstolar.is/default.aspx?pageid=347c3bb1-8926-11e5-80c6-005056bc6a40&id=3076afff-699c-4d3e-811d-e8fb87e9e32f and District Court of Reykjavik, Case No. E-3783/2015, 17 October 2016; link (official source): https://www.heradsdomstolar.is/default.aspx?pageid=347c3bb1-8926-11e5-80c6-005056bc6a40&id=4693e607-f791-45f4-bb3f-ae6758722aaf and District Court of Reykjavik, Case No. E-3784/2015, 17 October 2016; link: https://www.heradsdomstolar.is/default.aspx?pageid=347c3bb1-8926-11e5-80c6-005056bc6a40&id=31e3ef7d-7b6f-48a7-85b6-a74cb6bfbf95 .

[81] High Court of Ireland, Case No. 2008 1601 P ([2009] IECH 411), 24 July 2009.

[82] Supreme Court of Cassation, Judgement no. 49437, 23 December 2009.

[83] https://web.archive.org/web/20110612001810/http:/www.thestar.com.my/news/story.asp?file=%2F2011%2F6%2F11%2Fnation%2F8879884&sec=nation

[84] Court of Amsterdam, No. 428212 – KG ZA 09-1092, 30 July 2009, link (official source): https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2009:BJ4298, and Court of Amsterdam, No. 448310 - HA ZA 10-158, 16 June 2010, link (official source): https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2010:BN1626&, and District Court of The Hague, Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN) v. Ziggo BV, Case No. 365643 – KG ZA 10-573, 19 July 2010, link (official source): https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2010:BN1445&showbutton=true&keyword=brein+ziggo

[85] Borgating Court of Appeal, Nordic Records Norway AS v Telenor ASA, 9 February 2010.

[86] District Court of Lisbon, No 153/14.0YHLSB, 169605, 4 February 2015.

[87] Central Court of Administrative Litigation Madrid, N66028, 25 March 2015.

[88] Stockholm District Court, Case Name B 13301-06, and Swedish Patent and Market Court, Case No. PMT 7262-18, 15 October 2018.

[89] High Court of Justice, Chancery Division, Case No. HC11C04518 (([2012] EWHC 268 (Ch)], 20 February 2012.

material is usually quickly reposted on the site. The total number of visits of *Rarbg.to* between April 2017 and March 2018 was around 1.371 billion. The average rank worldwide was 304. 31% of the visits came from the EU, 69% from non-EU countries.

Rarbg.to has changed hosting services to prevent shutdowns in recent years. *Rarbg.to* reportedly generates income from advertisements and a pay-per-install distribution model for potential malware[90]. The website and its variants have been subject to blocking orders in Australia[91], Denmark[92], Finland[93], Ireland[94], Italy[95], Portugal[96] and the United Kingdom[97].

Rutracker.org

Rutracker.org is a BitTorrent website, which reportedly was launched in 2010 in response to the takedown of *Torrent.ru* by the Russian authorities. *Rutracker.org* has around 1,5 million active torrents and 13,9 million registered users. The site is hosted in Russia by a Seychelles company that is also reported by the film industry to be the operator of the site. The total number of visits of the site between April 2017 and March 2018 was around 968,1 million. The average rank of the site worldwide was around 325 during this period. The site has been subject to blocking orders in Russia[98].

Torrentz2.eu

Torrentz2 is a Bit Torrent website which allegedly emerged in 2017 following the closure of *Torrentz.eu*. It provides access to a range of content, including allegedly unauthorised copies of films, TV programmes, software, videogames and music. The site is currently hosted in Switzerland and is masked behind a reverse proxy service that curbs rightholders' ability to identify its precise host. The site positions itself as a new and improved version of *torrentz.eu*, searching over 80 torrent sites. The website also operates two mirror sites: *torrentz2.me* and *torrentz2.onion*. The site claims to currently index over 61 million torrents from 246 million pages on 81 domains. The total number of visits of the site between April 2017 and March 2018 was around 711,9 million. The average rank of the site worldwide was around 274. The website is blocked in Australia[99], Denmark[100], India[101] and Italy[102].

---

[90] *Symantec: Pay-Per-Install – The New Malware Distribution Network* - https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/security-response-pay-per-install-10-en.pdf

[91] Federal Court of Australia, No. NSD 269 of 2017, 18 August 2017.

[92] Court Frederiksberg, BS FOR-121/2015, 6 March 2015.

[93] Finish Court Case 311/18, link: https://www.markkinaoikeus.fi/fi/index/paatokset/teollisjatekijanoikeudellisetasiat/teollisjatekijanoikeudellisetasiat/1529045059067.html

[94] High Commercial Court, 2017 No 11701 P (2018 No. 6 COM).

[95] Italian Regulatory Authority for Communications, Decision 35/17/CSP; link (official source): https://www.agcom.it/documents/10179/6926764/Delibera+35-17-CSP/40e3701c-cf12-4662-b793-8899d767e4d0?version=1.0

[96] General Inspection of Cultural Activities (Inspeção-Geral das Atividades Culturais – Gabinete da Direção), 1101/IG/2015.

[97] London High Court of Justice, Claim No HC/2014/ 00466, Order 10 11 14 (5), 19 November 2014.

[98] Moscow City Court, Decisions No 3-726/2015 and No 3-0647/2015, link https://www.trademarksandbrandsonline.com/article/legal-update-rutracker-blocked-in-russia

[99] Federal Court of Australia, Case NSD 239 and 241 of 2016, 15 December 2016.

[100] Case Sag BS-906/2017-HRS, Rettigheds Alliancen som mandatar for KODA m.fl. mod Stofa A/S.

[101] The High Court of Delhi, CS(COMM) 724/2017.

[102] Italian Regulatory Authority for Communications, Decision 134/18/CSP, link: https://www.agcom.it/documents/10179/10838874/Delibera+134-18-CSP/d8526332-e70b-4076-b6cb-

1337x.to

1337x.to is a BitTorrent website which allegedly allows users to download films, TV programmes, games, music and apps. This BitTorrent indexing site is hosted in the US with possible ties to the Seychelles. This site is being masked behind a reverse proxy service that curbs the rightholders' ability to identify its actual host. Users are able to sort the content by genre, year and language. The main income of the website appears to originate from advertisements, but Bitcoin donations are also collected.

The total number of visits of *1337x.to* between April 2017 and March 2018 was around 958,8 million. The average rank of the site worldwide was around 493. 21% of the visits came from the EU, 79% from non-EU countries. The website is blocked in Austria[103] and Italy[104].

e) <u>Unlicensed pay per download sites</u>

Unlicensed pay per download sites engage in the unlicensed sale of music content at a significantly lower price than the licensed services. Even though these sites have the look and feel of legitimate download services with the official cover art, they are reportedly not licensed to use the content they offer.

Users usually create an account, add money to it and then search for the content they want to download directly from the website. The prices normally vary depending on the size of the file. These sites often offer also new releases.

As these sites allegedly do not pay royalties, they have presumably lower operation costs, thus likely competing unfairly with legitimate download services and reducing sales of licensed sites.

Mp3va.com and ***Mp3caprice.com***

According to the music industry *Mp3va.com* and *Mp3caprice.com* are popular unlicensed pay per download websites hosted allegedly in Ukraine, which provide mainly music. The total number of visits of *Mp3va.com* between April 2017 and March 2018 was around 156 million and of *Mp3caprice.com* around 27,6 million, with a worldwide rank of 64,308 and 257,497 respectively. Around 28% of the visits came from the EU, 72% from non-EU countries.

These sites claim to have a copyright licence for their business from the Ukrainian collecting society called AVTOR, which reportedly has no mandate to represent foreign rightholders.

51c90093ca8e?version=1.0

[103] Supreme Court of Austria, No. 4 Ob 121/17y, 24 October 2017, link (official source): https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=df3a2cab-8dd1-4ce4-8795-9cdfffc0e919&Position=1&Abfrage=Justiz&Gericht=&Rechtssatznummer=&Rechtssatz=&Fundstelle=&AenderungenSeit=Undefined&SucheNachRechtssatz=False&SucheNachText=True&GZ=4Ob121%2f17y&VonDatum=&BisDatum=09.11.2017&Norm=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=JJT_20171024_OGH0002_0040OB00121_17Y0000_000

[104] Italian Regulatory Authority for Communications, Decision 110/18/CSP; link: https://www.agcom.it/documents/10179/10452714/Delibera+110-18-CSP/ff89e9e8-ffa2-47ee-83b4-fd8e4af97a0d?version=1.0

f) Websites for Piracy Apps

Certain websites make available apps, which provide their users access to hundreds of pirated films and TV programmes. Once downloaded and/or registered/subscribed, Piracy Apps provide access to these pirated contents. Piracy Apps attract millions of consumers who often pay for subscriptions.

Popcorn Time

Popcorn Time is allegedly a Piracy App with high global audience numbers and is available in various forms and languages. The three most popular variants are *popcorn-time.to*, *popcorntime.sh* and *popcorn-time.is*. The websites are hosted in the US and they have ties allegedly to Russia and the US. Once installed, the users of the application have access to a huge library of films and TV programmes, allegedly made available without authorisation of the copyright holders. It is available for computers, phones, tablets and other portable devices. Courts in Belgium[105], Denmark[106], Italy[107], Norway[108] and the United Kingdom[109] have ruled that the application is illegal and has to be blocked by internet service providers.

g) Hosting providers

Pirate sites often depend on hosting providers that provide the necessary infrastructure for them to operate (for instance easy access or fast download). Thus hosting providers are in a good position to stop or prevent infringements.

Some hosting providers have policies against infringers and regularly take action to prevent their services from being used for copyright infringements, but there are others, which allegedly do not follow due diligence when opening accounts for websites to prevent illegal sites from using their services and do not cooperate with copyright holders in removing or blocking access to pirate content. These hosting providers often use Content Delivery Network (CDN) services[110] and thus provide anonymity to the operators of the pirate sites. CDN services are legitimate services, used also by legitimate businesses, but they are also often employed by pirate sites to hide the original IP address of the site which actually hosts the content (back host). The WhoIs Database[111] lists the IP address of the server within the CDN (front host) through which the content is routed and not the server actually hosting the content. The back host and its IP address are hidden by the CDN service. Therefore, in the WhoIs Database it is only possible to see the IP address of the server of the front host, but the IP address of the back host is hidden. These CDN service providers are attractive for infringing websites and are reported by the music, film and book publishing industry for not making enough efforts to facilitate removal of illegal content or blocking access to illegal

[105] District Court Mechelen, 2015/076, 20 October 2015.
[106] District Court of Frederiksberg, order: 969/2017; link: https://rettighedsalliancen.dk/wp-content/uploads/2018/03/BRFRB-05.12.17-Blokering-af-Popcorn-Time-1.pdf
[107] https://torrentfreak.com/court-orders-italian-isps-to-block-popcorn-time-150831/
[108] The Norwegian Economic Crime Unit (ØKOKRIM), 13 September 2017, link (official source): https://www.okokrim.no/inndrar-bruksretten-til-popcorn-time-no.6028617-411472.html
[109] High Court of Justice; Chancery Division [2015] EWHC 1082 (Ch), Case No. HC2014 – 002029, 28 April 2015.
[110] Content Delivery Network is a geographically distributed network of proxy servers and their data centres that improves the efficiency of the delivery of the internet content to end users.
[111] WHOIS is an online protocol that is widely used for querying databases that store registered data on the users of a domain name, the IP address, the name of the registrar, starting date and expiration date of the domain name, etc. The protocol stores and delivers database content to those using the protocol for searching.

websites.

CloudFlare

CloudFlare is a US based company, which provides hosting service combined with other services, including CDN services and distributed domain name server (DNS) services[112]. According to the creative industries (film, music, book publishers, etc.) and other organisations, *CloudFlare* is used by approximately 40% of the pirate websites in the world. It operates as a front host between the user and the website's back host, routing and filtering all content through its network of servers. Out of the top 500 infringing domains based on global Alexa rankings, 62% (311) are using CloudFlare's services, according to stakeholders. A sample list of 6,337 infringing domain names presented by the film industry showed over 30% (2,119) using CloudFlare's services.

CloudFlare provides anonymity to the owners and operators of the websites that use its services, which is particularly useful also for the operators of pirate websites. If the website uses CloudFlare, the IP address of the back host is replaced by one of CloudFlare's dedicated IP addresses and is therefore no longer ascertainable and CloudFlare reportedly does not easily provide information on the IP address of the back host.

According to the respondents, CloudFlare's cooperation with the rightholders, including CloudFlare's responsiveness to infringement notices should be improved (i.e. disabling access to its services and terminating accounts). Stakeholders also urge CloudFlare to follow due diligence when opening accounts for websites to prevent illegal sites from using its services and to strengthen its repeat infringer policy.

Private Layer

Private Layer is a company registered in Panama with servers in Switzerland, which serves as a front host also for infringing websites. Private Layer provides anonymity to the owners and operators of the websites that use its services, which makes them very attractive also for pirate sites. *Private Layer* is reported by the creative industries for hosting many IP infringing websites and for not having an effective policy to handle IP infringements. Stakeholders urge Private Layer to follow due diligence when opening accounts for websites to prevent illegal sites from using its services. According to the respondents, Private Layer's cooperation with the rightholders should be further enhanced, including its responsiveness to infringement notices (i.e. disabling access to its services and terminating accounts). The film industry indicated that they have sent more than 100 infringement notices and reminders on copyright infringing sites using Private Layer's hosting services in the last 3 years but reportedly these notifications were ignored.

h) <u>Ad-Networks</u>

Internet websites and mobile applications that provide access to services infringing IPR on a commercial scale use the sale of advertising space as one of their revenue sources. Advertising is a major source of income for digital piracy worldwide, and in many cases is the sole reason that pirate services can continue to operate. Brands are often unaware or are not in full control of where their advertisements are appearing because there are typically several

[112] Domain name server services are Internet services that translate domains names into IP addresses.

intermediaries[113] between them and the websites on which the ads ultimately appear[114].

The companies connecting advertisers to infringing websites contribute to the prosperity of infringing websites by providing funding to the operators of these sites through advertising revenue. Many Ad-Networks have established best practices and guidelines to reduce ads supporting or promoting piracy, others ignore IP infringements.

Some online ad networks and ad exchanges have joined the *Memorandum of Understanding on online advertising and intellectual property rights*[115] that brings together representatives of advertisers, advertising agencies, trading desks, advertising platforms, advertising networks, advertising exchanges for publishers, sales houses, publishers and IPR owners. The signatories of this MoU commit to minimise the placement of advertising on websites and mobile applications that infringe copyright or disseminate counterfeit goods on a commercial scale.

WWWPromoter

The Toronto-based *WWWPromoter* is - according to the music industry - the fastest growing advertising network used amongst infringing sites, which provide services among others to many pirate sites. By using *WWWPromoter's* services, operators of infringing sites are able to generate revenue from traffic and advertisements that the network directs to their site.

6. E-COMMERCE PLATFORMS

Electronic commerce offers numerous opportunities to increase consumers' choice and cross-border access to goods and services. However, even if the majority of trade on sales platforms is legitimate, e-commerce platforms also attract sellers who seek to distribute counterfeit goods. Some of the e-commerce platforms are being misused by such rogue merchants as a marketplace to deceive online shoppers. Consumers are led to believe that the product they buy is genuine, only to discover a counterfeit delivered to their homes[116].

The sale of counterfeit goods over the internet presents a threat considering that: i) consumers are at a growing risk of buying sub-standard and possibly dangerous goods, ii) the brand image and economic interests of European companies are damaged through the sale of counterfeit versions of their products, iii) the efforts of e-commerce platforms to be regarded as safe places to purchase legitimate products are undermined.

Against this background, the Commission *Recommendation on measures to effectively tackle illegal content online*[117] published on 1 March 2018 outlines certain principles and safeguards, which, in the interest of the internal market and the effectiveness of tackling illegal content online, and in order to safeguard the balanced approach that Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market[118] seeks to ensure, should guide the activities of the Member States and of the service

[113] Those intermediaries may include a media agency appointed by the advertiser, a trading desk, a demand side platform, ad auction system, supply side platform and an ad network.
[114] See *footnote 15*
[115] *Memorandum of Understanding on online advertising and intellectual property rights* https://ec.europa.eu/docsroom/documents/30226
[116] See *footnote 29*
[117] See *footnote 26*
[118] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML

providers in identifying, preventing reappearance and removing illegal content. The Recommendation identifies best practices, which online platforms are encouraged to follow in order to reduce the availability of illegal content, including counterfeit offers on e-commerce websites. The Recommendation aims in particular at clearer notice and action procedures, more effective tools and proactive technologies to detect and remove counterfeit listings and other illegal content, more transparency on online platforms and closer cooperation with trusted flaggers, rightholders and enforcement authorities.

During the public consultation for the preparation of the Watch List, the following main criteria for the selection of e-commerce and social media platforms to be included in the Watch List were identified: the estimated amount of counterfeit goods offered by them, the alleged low effectiveness of the measures to detect and remove counterfeit offers and/or the alleged insufficient level of cooperation with rightholders and enforcement authorities. Other factors reported such as the lack of clarity of the platforms' terms of service regarding prohibiting their use to sell or otherwise trade in counterfeit goods and services, the absence of effective vetting of the sellers who are trading on the platforms, or the non-use of effective automated risk management tools to identify high-risk behaviours and potential red flags were considered. On this basis, the Commission services identified the e-commerce platforms that are listed below.

Bukalapak

Bukalapak is the most popular online e-commerce platform in Indonesia, selling for instance electronics, clothing, fashion accessories, books, films, mobile phones, car and motor spare parts and industrial goods. Most of the commercial activity of the marketplace is business to consumer, but business to business activities are also common. Stakeholders reported that the platform sells a high number of allegedly counterfeit goods, mainly originating from mainland China. In 2017 the luxury industry reported 26,000 listings offering counterfeit goods on this platform. The marketplace has several revenue sources, such as advertising, cash-back[119] and premium accounts for the users.

According to a brand protection company using a machine learning software to uncover damaging threats to brands, the estimated counterfeit breakdown by sector is the following: 47% engineering and technology, 19% fashion and luxury, 17% sports, 12% tobacco and alcohol, 4% entertainment and 1% health and beauty. The processing time for removing infringing offers is deemed unreasonably long by stakeholders and there is no sufficient information as to whether the listings are removed or have simply expired. Stakeholders submit that the current web form for requesting a takedown only allows the attachment of images while submitting relevant documents such as letters from the authorities or trademark holders is not possible. The legal team of the platform occasionally states that the listings will be removed within 5-7 days, but they remain live. Stakeholders report that no proactive measures are applied to detect or remove the obviously counterfeit offers. Reportedly there is no prohibition of the use of contentious keywords in the listings, such as "replica". Due to the product categories offered via platform, the health and other consumer risks are also perceived to be high.

[119] An incentive for the buyers of certain products whereby they receive a cash refund after making a purchase.

***EVO Company Group (Tiu.ru**, **Prom.ua**, **Bigl.ua**, **Deal.by** and **Satu.kz**)*

The EVO Company Group manages marketplaces such as *Tiu.ru* (Russia), *Prom.ua* (Ukraine), *Bigl.ua* (Ukraine), *Deal.by* (Belarus) and *Satu.kz* (Kazakhstan). The most important ones respectively, in Russia and Ukraine, are *Tiu.ru* and *Prom.ua*. Stakeholders report that a high volume of allegedly counterfeit goods is readily available on these marketplaces and that the effort made by the operator to reduce the availability of these products is not satisfactory. The marketplaces range from business to business and business to consumer activities. The main product categories for sale on these marketplaces are car and motor spare parts, clothing, footwear and accessories, engineering and electronics, materials for repair, beauty and health, sport and leisure goods and books. According to a brand protection company using a machine learning software to uncover damaging threats to brands, the estimated counterfeits breakdown by sector is the following: 52% fashion and luxury goods, 36% engineering and technology while the rest is divided amongst sports, entertainment, tobacco, alcohol, health and beauty products.

For takedown, the marketplaces require an official complaint with all the infringing URLs to be printed out, signed and stamped by the company representatives. The scanned documents are then sent via email for assessment. Only trademarks registered in the home country of the marketplace are accepted. Processing of a complaint reportedly often takes several weeks and these platforms are not responsive to requests for updates. Once the requests for takedowns are processed, sellers are given 5 days to remove the reported listings. Failure to do so is intended to result in takedowns by the marketplaces. However, the platforms are reportedly very inconsistent in taking action.

The main obstacles to tackle the high number of alleged counterfeits available on these marketplaces is the time-consuming process of reporting counterfeit products, the lack of responsiveness by the respective legal teams by email and the rejection of international trademarks registered at WIPO and designated to the host country of the marketplace. In addition, the platforms frequently leave reported listings online without communicating the reason for doing so.

Lazada.co.th

Lazada is one of the most popular online e-commerce (business to consumers) platforms in Thailand, which was reported by the European sporting goods, luxury and automotive industries, as well as by fashion brands and associations fighting against counterfeiting, due to the high volume sale of allegedly counterfeit sports goods, clothing, footwear, car and motorcycle spare parts, electronic devices and accessories, jewellery and luxury goods. Stakeholders also reported on barriers to take down counterfeit goods, including low level of responsiveness, unreasonably stringent enforcement requirements, long processing times and inconsistencies in handling complaints.

In addition, they reported on shortcomings with regards to proactive detection, identification and removal of counterfeit listings, a weak system for vetting of sellers, as well as on insufficient cooperation with rightholders and the lack of investment in, and use of, automatic detection technologies.

Naver.com

One of the major online e-commerce platforms in Korea is operated by *Naver Corporation*.

According to stakeholders counterfeit goods are offered through *Naver Corporation*'s shopping and social media services, including *Naver Window Series* (an online open market platform for offline store operators) and *Smartstore* (a platform for online shop operators).

Stakeholders, mainly from the luxury and fashion industry, reported that counterfeit goods can be easily found on *Naver Blogs*, *Naver Cafes*, and *Naver* shopping platforms by typing various keywords. Reportedly there is no prohibition of the use of contentious keywords in the listings. Searches for blatant terms (i.e. "replica" in Korean and English) and terms implying the products' counterfeit nature ("A-class" and "mirror-class" in Korean) resulted in a high number of hits on *Naver Window Series* and *Smartstore*. The European Chamber of Commerce in Korea reported that a total of close to 50,000 notice and takedown requests were submitted to *Naver Corporation* by only 12 companies in 2017 alone, which, according to the Chamber of Commerce, illustrates that *Naver* needs to improve its detection, and removal techniques, in order to decrease the sale of counterfeit products on its platforms. Better cooperation with trusted flaggers and rightholders in general would potentially also improve the situation.

Snapdeal.com

Snapdeal is one of the most popular online e-commerce (business to consumers) platforms in India, which was reported by stakeholders for the high volume of allegedly counterfeit goods offered on the platform.

According to stakeholders, the platform's policies against IP infringements and for the detection and removal of illegal listings are not properly implemented; the vetting of sellers and the use of proactive measures to detect illegal listings are not sufficiently effective. Although *Snapdeal*, in its policy statement, commits to take down IP infringing listings upon adequate notification and to work with various brand owners to delist or bar from the platform sellers who have been identified by the brand as selling counterfeit goods, it is reportedly not implemented consistently in practice.

Snapdeal uses an image recognition system that helps identifying apparent violations but according to stakeholders other automatic technologies are also needed, as they could help to analyse and correlate product, price and image related information to flag suspicious listings for further analysis.

Xxjcy.com and China-telecommunications.com

Xxjcy.com and *China-Telecom* are China-based business to business marketplaces, where the suppliers are enterprises registered in China. The platforms offer industrial products and supplies for sale as well as consumer goods. Stakeholders report that a high volume of counterfeit construction machinery, chemical machinery, clothing, engine parts, fashion accessories, textile products, lights and lighting products and furniture are readily available for retailers. According to the stakeholders, there is a potential risk for the counterfeit goods to be resold on European marketplaces, given that the products are sold in large volumes and international shipping is available. Both *China Telecommunications* and *Xxjcy* are assumed to be linked, because they have exactly the same adverts and layouts when searching keywords across the platform (also with other platforms such as *Chinatele*, *Esadidasol* and *Everychina*). Users are not able to purchase through the sites, instead, they are given the option to contact the seller to make purchases outside of the platforms.

According to a brand protection company using a machine learning software to uncover damaging threats to brands, the estimated counterfeits breakdown by sector is the following for the two marketplaces respectively: 53 and 59% engineering and technology, 18 and 19% sports goods, 11 and 16% fashion and luxury, 8 and 10% entertainment and the rest divided among tobacco, alcohol, health and beauty products.

The platforms provide a web form to send notices for the removal of counterfeit goods. According to the stakeholders, the platforms do not act on complaints at all, are not responsive to notifications and enforcement through the web form has not resulted in any takedowns.

Ongoing efforts to reduce the offer of counterfeit goods

Besides the platforms listed above, in the course of the public consultation, a number of stakeholders reported other platforms (*Aliexpress.com*, *Tmall.com*, *Taobao.com*, *1688.com*[120], *Amazon.com*[121] and *eBay.com*[122]) where, stakeholders maintain that, despite efforts, a significant volume of allegedly counterfeit goods is offered. At the same time, it was also reported that these platforms' level of compliance with the *Recommendation on measures to effectively tackle illegal content online*[123] was much higher than that of the above listed e-commerce platforms. It was also stressed that the operators of these platforms are generally open to cooperate with rightholders, including as signatories of the *Memorandum of Understanding on the sale of counterfeit goods via the internet*[124]. Taking this into consideration, these platforms are not listed on this Watch List. It is noted, however, that according to stakeholders further progress is needed to ensure that offers of counterfeit products disappear from these platforms or are significantly reduced.

More specifically, stakeholders report that these platforms apply both proactive and reactive measures to detect and remove counterfeit offers and apply terms of service that include IPR protection policy prohibiting the use of their platforms to sell counterfeit products or to provide other infringing services. According to stakeholders, these platforms apply a number of good practices to enforce the terms of service *vis-à-vis* traders and to cooperate with rightholders. These good practices include, for instance, tools allowing rightholders to register their brands, report counterfeit listings and fast-track take down procedures. Some of these platforms also partner more closely with brand owners and content creators to optimise detection models. Moreover, these platforms apply different technological measures, such as automated risk assessment tools, image recognition and semantic recognition algorithms seeking to reduce the availability of counterfeit offers as well as item-tracing authenticity services to help consumers verify the authenticity of products.

Despite these good practices, stakeholders indicate that allegedly counterfeit goods damaging mainly the fashion, leather, luxury, car, sports and creative industry (illegal streaming devices) are relatively frequently available on these platforms. Stakeholders report that cooperation with the rightholders should be further enhanced, for instance, by simplifying access to the brands' registers. Stakeholders also urge these platforms to improve their traders' vetting systems and to adopt or improve automated risk management and detection tools to identify

[120] Platforms operated by *Alibaba*
[121] Platform operated by *Amazon*
[122] Platform operated by *eBay*
[123] See *footnote 26*
[124] See *footnote 29*

high-risk behaviours and potential red flags, including dealing with repeat infringers and suspicious offers. According to the contributions received, the responsiveness of these platforms to the takedown requests and the consistency in dealing with similar cases should also be improved. In particular, the stakeholders reported that the following indicators are not sufficiently relied on by the platforms when proactively identifying suspicious listings: unusual low price level and overly long shipping time, sellers' history and feedback, lack of pictures of actual products offered (e.g. unauthorised use of catalogue pictures, use of pictures that are not showing labels of the product) and absence of information in the listing description. The lack or low quality of pictures and no information in the description often makes it impossible for brand owners to determine the authenticity of the products.

7. ONLINE PHARMACIES AND SERVICE PROVIDERS FACILITATING THE SALES OF MEDICINES

The sectoral study of the European Union Intellectual Property Office (EUIPO) on the economic cost of IPR infringement in the pharmaceutical sector[125] shows that 4,4% of legitimate sales of medicines (around EUR 10,2 billion) are lost each year in the EU due to counterfeiting.

The sectoral study also confirms that a further EUR 7,1 million is lost yearly in related sectors and 37,700 jobs are directly affected across the pharmaceutical sector in the EU, as legitimate manufacturers and distributors of medicines employ less people due to counterfeiting. Additional 53,200 jobs are lost in related sectors in the EU. According to this study the total yearly loss of government revenue as a result of counterfeit medicines in this sector across the 28 Member States in terms of household income taxes, social security contributions and corporate income taxes is estimated at EUR 1,7 billion[126]. In addition, based on data for the period 2011-2013, fake medicines sold in non-EU countries cost the EU pharmaceutical sector EUR 3,3 billion annually or 3,4% of total EU exports.

As e-commerce booms, the availability of medicines online has increased. Consumers are often deceived and buy counterfeit and falsified medicines. Counterfeit medicines range from lifestyle medicines to life-threatening counterfeit cancer medication and hormones. Counterfeit medicines may contain too little, or too much, or none of the active ingredient contained in the genuine medicine, may have been manufactured under unsanitary conditions and may contain contaminants. Consequently, the consumer threat and product safety risks are extremely high when it comes to counterfeit and falsified medicines. According to a study by the World Health Organisation (WHO)[127], over 50% of the medicines sold online are reported to be counterfeit.

Illicit online pharmacies play the biggest role in online distribution of counterfeit medicines, but occasionally also online sales platforms sell counterfeit medicines. To address the concern of illegal online sales of medicines in the EU, the Falsified Medicine Directive 2011/62/EU[128] has introduced specific provisions to increase the safety of online purchases of medicines. According to these provisions, all online pharmacies or retailers legally operating in the EU

[125] *The economic cost of IPR infringement in the pharmaceutical sector* https://euipo.europa.eu/ohimportal/en/web/observatory/ipr-infringement-pharmaceutical-sector
[126] See *footnote 125*
[127] *Growing threat from counterfeit medicines – Bulletin of the World Health Organisation* http://www.who.int/bulletin/volumes/88/4/10-020410/en/
[128] https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/dir_2011_62/dir_2011_62_en.pdf

are required to display a common logo, which provides a link to the website of the national competent authority listing all legally operating online pharmacies or retailers in the Member States concerned. Moreover, online pharmacies may only sell the products complying with the legislation of the Member State of destination and the Member States can impose additional conditions for the retail supply of medicinal products on their territory. In parallel, the Commission Delegated Regulation (EU) 2016/161 laying down detailed rules for the safety features appearing on the packaging of medicinal products for human use sets up an end-to-end verification system for prescription medicines[129]. The new rules require that online pharmacies in the EU verify the authenticity of prescription medicines and check if they have not been tampered with before supply to consumers or patients. The risk of counterfeit and falsified medicinal products from illegal websites nevertheless remains high.

According to the 2016 Study published by Legiscript[130], globally only 4% of internet pharmacies operate lawfully. The estimate is that around 30,000-35,000 illicit online pharmacies are active on the internet and fail to adhere to applicable legal requirements, sell prescription medicines without requiring a valid prescription or sell counterfeit, falsified or substandard medicines.

According to the European pharmaceutical industry, the typical rogue network model includes customer service call centres, back-end merchant accounts with acquiring banks and a medicine distribution system. The operators of illicit online pharmacies usually own clusters of hundreds of websites, some of which are the anchor websites where the actual sales take place. Most of them are websites that funnel internet users back to the anchor websites, while the rest are sleeping websites used only when an active website is shut down by the enforcement authorities. The websites are promoted through search engine optimisation and email spams.

Illicit online pharmacies also advertise and sell genuine medicines from well-known pharmaceutical companies (i.e. using copyright-protected pictures and registered trademarks) on their websites, but the European pharmaceutical industry reported that counterfeit medicines could be also obtained from the same website posing a grave threat to consumers' safety. The following domain names are examples for websites, which were reported by stakeholders as belonging to illicit pharmacy networks, which offer for sale and deliver also to the EU allegedly counterfeit and falsified medicines: *modafinil4uk.com*, *modapharma.com*, *mymedsalltime.com*, *chemstorex.at* and *alphabettermedshop.com.*

In addition, the European pharmaceutical industry reported that some rogue domain name registrars also facilitate the business of illicit online pharmacies. Most registrars limit access to illicit online pharmacies when they are notified of IP infringements by pharmaceutical companies. These prudent domain name registrars have a policy in place to prohibit domain names to be used for illicit activities. When they are notified of an alleged IP infringement, they suspend the domain name so that the site is no longer accessible to the public. However, some domain name registrars reportedly do not enforce any policy against counterfeit medicines.

[129] Commission Delegated Regulation (EU) 2016/161 supplementing Directive 2001/83/EC of the European Parliament and of the Council by laying down detailed rules for the safety features appearing on the packaging of medicinal products for human use https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_2016_161/reg_2016_161_en.pdf

[130] *The Internet Pharmacy Market: Trends, Challenges and Opportunities* http://safemedsonline.org/wp-content/uploads/2016/01/The-Internet-Pharmacy-Market-in-2016.pdf

Considering the high number of illicit online pharmacies and the fact that they operate anonymously, the Watch List focuses in this section on a few domain name registrars. These domain name registrars are based outside the EU and according to the European pharmaceutical industry are non-responsive to abuse notifications and are often used by rogue online pharmacy networks that offer to deliver medicines also to EU Member States.

CJSC Registrar R01 (registrar) **serving *EVA Pharmacy, PharmCash online pharmacy networks***

CJSC Registrar R01 is a domain name registrar that reportedly serves many rogue internet pharmacies. It provides domain name registration services to *EVA Pharmacy and PharmCash*, which are reportedly illicit online pharmacy networks offering for sale counterfeit medicines as well as prescription medicines without requiring the prescription. These networks use many referral[131] websites. Almost all of the active websites affiliated with these networks redirect users to a less visible online pharmacy website. The use of referral internet pharmacies allows the continuous operation of the network, because their redirection patterns can be changed easily anytime, including when a destination anchor online pharmacy has been suspended or disabled.

A joint industry initiative led by the Pharmaceutical Security Institute (PSI) in 2017[132] targeted *Eva Pharmacy* and *PharmCash*. Abuse and cease and desist notices were sent out to 172 websites operated by *EVA Pharmacy* and 587 websites operated by *PharmCash*. Many of these still active websites are served by the *CJSC Registrar R01* from Russia (22 websites from *EVA Pharmacy* and 102 websites from *PharmCash).*

The following registrars were reported for serving these and other illicit online pharmacy networks and for not cooperating with rightholders in disrupting illicit online pharmacy networks: *Registrar of Domain Names Reg.Ru, Regtime Ltd* and *R01-RU* from Russia, *GKG.Net* from the United States, *Paknic Private Limited* from Pakistan and *Afriregistar* from Burundi.

EPIK Inc. *(registrar)* **serving *RxProfits* online pharmacy network**

EPIK Inc. is a domain name registrar, which - according to the European pharmaceutical industry - provides domain name registration services to, among others, illicit online pharmacies, such as *RxProfits* network. *RxProfits* is an internet pharmacy network that offers allegedly counterfeit medicines (and prescription medicines to consumers without requiring a prescription). This network always uses referral websites. Almost all the active websites (99%) affiliated with *RxProfits* redirect users to a less visible internet (anchor) pharmacy website, the *pharmacy-xl.com*. This anchor website processes transactions for approximately 500 networked referral internet pharmacies. In addition to offering worldwide shipping, the network actively advertises some controlled substances, including *Xanax, Valium, Soma, Ambien,* and *Tramadol*.

A joint industry initiative led by the Pharmaceutical Security Institute[133] in May 2018 targeted 500 *RxProfits* websites by sending out abuse and cease and desist notices to its websites (registrants), its ISPs and registrars. *RxProfits* largely uses *EPIK Inc.* which is based in the

[131] See *footnote 40*
[132] http://www.psi-inc.org/index.cfm
[133] See *footnote 132*

United States. More than 60% of the current non-compliant websites are registered with *EPIK Inc*. When notices were sent out, only 33 *EPIK* sites were terminated.

ZhuHai NaiSiNiKe Information Technology Co. *(registrar)* **serving *PharmaWeb* online pharmacy network**

ZhuHai NaiSiNiKe Information Technology is a domain name registrar, which - according to the European pharmaceutical industry - provides domain name registration services allegedly to, among others, illicit online pharmacies, such as *PharmaWeb* network. *PharmaWeb* is an internet pharmacy network that reportedly offers counterfeit medicines and has connections to Canada. The network mostly targets the US market, but the medicines sold are distributed from countries outside the US, including, Italy, South Africa, New Zealand, India, the United Kingdom, Israel, Switzerland, Fiji and Canada. Although the network markets itself as a Canadian pharmacy, consumers using a Canadian IP address cannot access these websites. Blocking access from the country in which the operation is based is a common tactic used by illegal pharmacies networks.

PharmaWeb was targeted by a joint industry initiative led by the Pharmaceutical Security Institute[134] in June 2018. Abuse and cease and desist notices were sent out to 89 websites. Only 9 websites complied and are offline. 56 out of the 80 still active websites are provided domain name services by registrar *ZhuHai NaiSiNiKe Information Technology* from Hong Kong, which reportedly does not cooperate with rightholders. According to stakeholders, it reflects the link with illicit online pharmacy networks such as *PharmaWeb*, which relies disproportionately on non-compliant registrars.

8. PHYSICAL MARKETPLACES

Despite the boom of e-commerce, the sales of counterfeit goods in physical marketplaces continue to be widespread around the world. Physical marketplaces offer both high and low quality counterfeit goods[135]. Many of the physical marketplaces reported by stakeholders are located in areas frequented by tourists, others are frequented mostly by locals.

Argentina

La Salada, Buenos Aires

La Salada is situated in Buenos Aires and is allegedly one of the biggest marketplaces of counterfeits in Latin America. It is located in an area of more than 20 hectares where over 15,000 stands sell all kinds of products, most of them allegedly counterfeit. *La Salada* is divided into three sub-marketplaces: *Ocean*, *Hurkupiña* and *Punta Mogotes*, each one of which has its own administrators and rules. None of these sub-marketplaces seem to have rules strict enough to prevent or deter counterfeiting and other illegal activities. Most of the counterfeit products are allegedly imported from China, but some local assembly may also take place in the neighbourhood. Besides, it is reported that there are over 40 allegedly illegal clothing factories in *La Salada* and its close neighbourhoods.

[134] See *footnote 132*

[135] As described in the EUIPO study *Mapping the economic impact of trade in counterfeit and pirated goods*: "*In primary markets, prices are expected to be close to those of legitimate products, whereas larger price dispersions are expected in secondary markets. Consumers that knowingly purchase an IP infringing product may expect to pay a lower price for it than for a genuine product*".

As from 2016, local authorities seem to have started to intensify efforts against counterfeiting on this market leading to several police raids, the seizure of high volumes of counterfeit goods and the arrest of two suspect leaders of the market, along with some associates. Despite these raids, illegal activities and counterfeiting reportedly continue flourishing on the market and further actions and continued efforts are needed to cleanse this marketplace from counterfeiting.

Canada

Pacific Mall, Markham

The *Pacific Mall* is situated in Markham, Ontario and is one of the biggest shopping malls in Canada, which allegedly offers for sale a high volume of counterfeit clothes, footwear, toys, car spare parts, cameras, cell phones, computers and other electrical appliances, cosmetics, perfumes, health and beauty products, houseware, jewellery, watches and optical products. It covers around 25,000 square metres and has around 500 retail shops selling allegedly mainly counterfeit goods of Chinese origin.

After *Pacific Mall* had been put on the US notorious markets list in 2017, the owners reportedly made preliminary steps to tackle counterfeiting. These steps included for instance issuing written warnings to store owners and tenants engaging in counterfeiting. *Pacific Mall* also partnered up with manufacturers to help identify counterfeit goods and hired a private investigator to conduct internal audits and other checks in the premises of the merchants. Shoppers can report goods suspected of infringing IP rights via a dedicated website. Lease contracts have been amended and notices have been given to those caught on selling counterfeit products.

Despite these efforts, the scale of counterfeiting on this marketplace reportedly continues to be high and both the operators and the local authorities are urged by the stakeholders to take further actions in order to reduce the availability of counterfeit goods.

Other marketplaces in Canada, such as *Dixie, Weston*, *Dr. Fleas Flea Markets* and *Downsview Park Merchants Market* in Toronto, *Saint Eustache Flea Market* in Quebec as well as *747 Flea Market* in Brampton, Ontario were also reported by stakeholders for the sale of massive amounts of counterfeit goods.

China

Huaqiangbei Electronics Markets, ***Shenzhen* (*Yuan Wang Market, Manhar Digital Plaza, Longsheng* Market and *Mingtong Market*)**

There are dozens of multi-storey shopping complexes filled with distributor shops in *Huaqiangbei* District in Shenzhen that is a central hub for allegedly counterfeit consumer electronics. Buyers travel to *Huaqiangbei* to buy directly from these markets or order products to be shipped to their home countries.

Almost all kinds of allegedly counterfeit electronics and accessories (in particular phones) are produced in Shenzhen or elsewhere in Guangdong Province. These alleged counterfeits are then shipped globally through ports in Shenzhen and neighbouring Hong Kong and sold to

consumers as genuine goods also in the EU. Chinese enforcement authorities, particularly from the Public Security Bureau (PSB), work with brands to conduct raids in factories and distributors throughout China, and even pursue complex cross-border cases and inter-agency prosecutions.

Despite the raids, the *Huaqiangbei* tech malls reportedly conduct counterfeit sales. Even when the brands convince authorities to take action, the mall management and shop owners do not cooperate. As a result, counterfeiting reportedly persists with little actual deterrence. Particularly problematic *Huaqiangbei* tech malls which were reported by the stakeholders: *Yuan Wang Market*, *Manhar Digital Plaza*, *Longsheng Market* and *Mingtong Market*.

Asia Pacific Xingyang Fashion and Gifts Plaza and Asia Pacific Shenghui Leisure and Shopping Plaza, Shanghai

These two plaza marketplaces are in Pudong District in Shanghai and reportedly sell high volume of counterfeit clothes and accessories, cosmetics as well as footwear from many European and other brand owners. The two markets are interlinked and operated by the same landlord and stakeholders report that sellers tend to openly characterise their products as high quality genuine goods showing intent to deceive consumers.

Rightholders report that almost all the goods are counterfeit and authorities rarely perform any raids in these markets. Ban notices have been posted in the plaza warning against IP infringement. Representatives of the landlord have carried out inspections with lawyers and demanded some tenants to immediately remove counterfeits, but these efforts are considered not enough to reduce the availability of counterfeit goods on these marketplaces. Rightholders have investigated and have taken enforcement actions against some sellers in these plazas, but these efforts have not led to the reduction of the sale of counterfeit goods.

Anfu Market and its neighbourhood, Putian City

Anfu Market and its neighbourhood in Putian City (and the city itself) in Fujian Province in China is reportedly the centre of counterfeit shoes. Besides, *Anfu* Market sells also allegedly counterfeit luxury goods and clothing. *Anfu* Market is open only during the night. The merchants of *Anfu* Market do not only receive orders from retailers, but also engage in online sales and allegedly sell expensive counterfeits. Many counterfeit shoes sold on Chinese and other sales platforms are allegedly from *Anfu* Market.

According to the European sports goods industry, the places where the counterfeit goods are manufactured and stored before distribution on *Anfu* Market and on other marketplaces are mainly concentrated in *Licheng District* (mostly in *Huangshi town*, *Qibu village*, *West Tianwei town*), *Chengxiang District* (mainly *Huating Industrial Park*) and *Xiuyu District*. Among the local factories around 20% are large-scale factories with a daily output of about 500-2,000 pairs of allegedly counterfeit shoes, 50-60% are allegedly medium-sized workshops with an output of about 500-1,000 pairs daily.

Stakeholders report that due to local protectionism it is difficult to take actions against counterfeiters in *Anfu* Market and its neighbourhood. The local authorities are reportedly not responsive to rightholders' complaints and there are not enough raids to significantly reduce the availability of counterfeit goods on this market. To mitigate the risk of raids, factories usually ship all the products to a nearby warehouse after the production is complete or the

manufacturers split the production process into different steps and each step is finished in different workshops.

Mule Town in Guangxi Province

Located in the eastern part of Guiping City, *Mule Town* is the famous "Chinese Leisure Sportswear Village". Stakeholders report that manufacturing and selling counterfeit sportswear are its main economic pillar. The main products sold in *Mule Town* are jerseys of popular football teams and World Cup national jerseys.

Many counterfeit garment factories are reportedly located on the east side of the town, mainly concentrated in the industry zones (around 35 factories are allegedly in the area). On the west side the garment factories are more dispersed. Reportedly, only a small number of large factories keep 10,000-20,000 sets of counterfeit sportswear in stock, the rest adopted a safer approach, namely that while fabric cutting and processing are done inside the factories, neighbouring workshops manufacture the finished products. At night, the finished products are transported to warehouses in rural areas for storage. Warehouses are usually located in Zhenlong Town or Gaotang Village. Stakeholders report that at night trucks stop at each station and load counterfeit products, driving through the S304 provincial highway to Guangwu express way or S40 Cangshuo express way, finally reaching Guangzhou City, where products are distributed.

Chengdu Qinglong Shoes Wholesale Markets in Jinniu district, Chengdu and Shangmeicheng Market at Chunxi Road, Wuhan

Chengdu Qinglong Shoes *Wholesale Markets* in Jinniu district and *Shangmeicheng Market* at Chunxi Road have a large stock of counterfeit shoes of poor quality according to the European sports goods industry. There are also discount sale booths in the downtown area of Chengdu and Wuhan, near to the authorised stores of European sports brands. They reportedly sell counterfeit products at a relatively low price and attract many customers who mistakenly take their products to be genuine. There are reportedly also many "Fake Franchise Stores" in the same downtown areas around the listed markets, some stores replicate the store design of reputed European brands and allegedly sell only counterfeit goods. Peddlers reportedly hide counterfeit goods in residential areas near the pedestrian area in the downtown, stand in front of the authorised stores of European sport brands, grab consumers and take them to their booths to sell them counterfeit products of low quality at a much cheaper price. Stakeholders report that these merchants deceive consumers and run the business with impunity. The majority of these discount sales booths and Fake Merchandise Stores allegedly purchase part of their supplies from the listed wholesale markets.

Discount sale booths are usually open only for a few days, typically during holidays or weekends. Consequently, the authorities are perceived to not respond sufficiently quickly to the rightholders' complaints. It has been reported that infringers come back quickly after enforcement actions took place. Local authorities are perceived to not impose severe punishment on these infringers and thus to not deter repeated infringers.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in China, for instance on *Dajingkou Shoes and Clothing Market* in Qingyang Town, the *Silk Market*, *Shenyang Wu Ai Market*, *Guangzhou Baiyun World Leather Trading Center* and *Luohu Commercial City*.

India

Karol Bagh Market, Tank Road Market and Gaffar Market, Delhi

Many marketplaces located in India were reported by stakeholders for selling counterfeit sports goods, footwear, clothing, apparel, luxury goods, watches and cosmetics. The three listed marketplaces are just examples of the many markets in India, where reportedly counterfeit products such as apparels, watches, footwear and eyewear are sold both at wholesaler and retailer level. These are well-known markets in Central Delhi and several European brands have opened shops around these markets and reported counterfeiting of their brands on these marketplaces.

According to stakeholders, some civil and criminal enforcement actions have been taken resulting in successful seizures of counterfeits, which however has not proved to be effective enough. Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in India, for instance on *Lajpat Rai Market*, *Arya Samaj Road* and *Hardiyan Singh Road* markets as well as *Sarojini Nagar* market in Delhi, the *Crawford Market* in Mumbai, *Khidderpore* market in Kolkata or the *Sector 18, Atta Market* in Noida as well as *Akal Garh*, *Chaura Bazar*, *Mochpura Bazar*, *Gur Mandi* Markets in Ludhiana.

Indonesia

Mangga Dua Market, Jakarta

Mangga Dua Market is a well-known marketplace, located in Jakarta, Indonesia. The market reportedly offers a broad variety of counterfeit goods such as handbags, fashion accessories and clothing. Retailers reportedly buy high volumes of cheap counterfeit goods on this market to sell them afterwards for a deceptively high price in other markets or retail shops.

Korea

Dongdaemun Special Tourist Zone, Seoul

The *Dongdaemun Special Tourist Zone* has wholesale shopping malls and traditional malls but it has also become a hub for street sellers and operators of stores mostly for apparel-related goods, featuring 150,000 merchants daily. The zone reportedly also sells counterfeit products in high volume. The main operating hours of the street stalls reportedly selling counterfeit products are at night, hampering proper enforcement. As a response to the enhanced enforcement activity of the Seoul Central District Office's Counterfeit Crack Down Task Force, stakeholders report that many merchants now tend to conduct covert sales of counterfeit products.

The Seoul Central District Office and the European industry in 2013 established a joint action aimed at increasing enforcement activities against the sale of counterfeit goods on this market. After being designated with special judicial authority, five local government officials conducted raids against merchants selling counterfeit products on this market. The raids resulted reportedly in a steep drop in the number of street stalls selling counterfeit goods. From the start of the initiative until the end of 2017, the regional authorities responsible for *Dongdaemun* conducted many seizures. More than 70% of these seizures were undertaken in

the *Dongdaemun Special Tourist Zone*. According to stakeholders, the activities of the Seoul Central District Office's Counterfeit Crack Down Task Force have also resulted in a large decrease in street stalls selling counterfeit products.

Despite the continuous efforts of the enforcement officials and the high standard enforcement regime of Korea, stakeholders report that the sale of counterfeit products on the *Dongdaemun Special Tourist Zone* still persists.

Malaysia

Petaling Street Market, Kuala Lumpur

The *Petaling Street Market*, which is located in Kuala Lumpur in Malaysia, is a major tourist attraction, which reportedly remains a marketplace for counterfeit goods. High volumes of allegedly counterfeit clothing, footwear, handbags and perfumes are for sale in this market, some of them are high quality, expensive, showing intent to deceive consumers.

Only very minimal raid actions appear to be possible due to alleged lack of manpower in the enforcement authorities. Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in Malaysia, for instance on *Taman Johor Jaya* market in Johor Bharu, the *Berjaya Time Square* market, *the Jalan TAR* open market, the *Low Yat Plaza* and the *Tamaran Johor* market in Kuala Lumpur as well as the *Batu Ferringhi* Night Market in Penang.

Mexico

El Tepito, Mexico City

El Tepito is an open-air market and trading hub in Colonia Morelos in the Cuauhtémoc borough of Mexico City, which, according to stakeholders, is dedicated to the production, storage and wholesale and retail distribution of all sorts of counterfeit goods. Stakeholders report that it is difficult for the enforcement authorities to control this market.

Stakeholders reported that *El Tepito* market has become increasingly dangerous, making it almost impossible for rightholders to enforce their rights. Allegedly, most of the counterfeit goods come from China, stored in a labyrinth of tunnels and secret warehouses and the goods are not only sold on this market but distributed throughout Mexico and other countries. Despite the success of some raids, in most cases the merchants allegedly revert soon to sale of counterfeits.

San Juan de Dios Market, Guadalajara

San Juan de Dios Market is one of the biggest indoor markets in Latin America, with an area of 40,000 square metres and with more than 3,000 stalls. The market is located in the centre of Guadalajara, in the Mexican State of Jalisco. Stakeholders report that around 50% of the stalls sell counterfeit apparel, electronic appliances, footwear, jewellery and watches as well as CDs and DVDs.

The enforcement authorities have apparently conducted several raids against rogue merchants on the market, but the reaction of the sellers may be violent. It was reported that at least on

one occasion the Mexican Army needed to provide security to avoid further incidents. Stakeholders report that taking action with the support of the state authorities of Jalisco or the municipal authorities in Guadalajara is practically impossible.

Russia

Gorbushkin Dvor Mall, Moscow

The *Gorbushkin Dvor Mall* in Moscow is one of Russia's highest profile "tech malls". It has become a well-known outlet for cheap consumer electronics and household appliances, but allegedly counterfeit perfumes, clothes and fashion accessories are also readily available on this market. Many of the stores are also using unauthorised branding to advertise their stores and goods. Stakeholders report that the majority of the goods sold on this market come from China through the Russia-Kazakhstan border.

Stakeholders report that enforcement in *Gorbushkin Dvor Mall* has been almost impossible and that complaints sent by rightholders are usually ignored. Obtaining evidence through covert investigations has been dangerous and reportedly the local police do not carry out raids on any premises on this market. Up until recently, brand owners were discouraged from filing criminal complaints.

The *Dubrovka Market* in Moscow was also reported by stakeholders for the massive amount of counterfeit goods.

Thailand

MKB Center, Bangkok

MKB Center, also known as *Mahboonkrong* is a shopping mall in Bangkok, which has more than 2,000 shops allegedly selling high volume of counterfeit clothing, accessories, electrical appliances (computers and cell phones), cosmetics, beauty supplies, entertainment, footwear, jewellery and watches. Stakeholders, including the European sports goods industry reported that in *MKB Center* around 100-500 counterfeit goods per shop are readily available with further stock places nearby.

The problem is known by the local Thai authorities (the Department of Intellectual Property, the Thai Royal Police and the Thai Royal Army) who worked closely together to conduct *ex-officio* raids in counterfeit marketplaces in Bangkok in June 2017 and during this operation over 5,000 counterfeit goods of different brands were seized in the *MBK Center*. The authorities work with the landlord in suppressing counterfeit goods and the Department of Intellectual Property has set up a working group to tackle the problem of IP infringements. Despite these efforts, the *MKB Center* allegedly continues to be home to both high and low quality counterfeit goods.

Massive amounts of counterfeit goods were also reported by stakeholders on other marketplaces in Thailand, for instance in the *Mike Shopping Mall* in Pattaya, the *Patpong Night Market* and *Chatuchak Market* in Bangkok, *Shops and Stocks around Patong Beach* in Phuket and *Phuket Night Market*, *Fisherman's Village Walking Street Market* in Bophut, *Lamai Walking Street and Night Plaza* in Maret, as well as in the *Rong Kluea Market* in Sa Kaeo.

Turkey

Grand Bazaar, Istanbul

The *Grand Bazaar* is one of the largest and oldest covered markets in the world, located in the centre of Istanbul, with 61 covered streets and over 4,000 shops which attract between 250,000 and 400,000 visitors daily. It allegedly sells, among others, counterfeit handbags, watches, cloths, perfumes, leather goods and toys, adjusting the prices to the tourists' wallets. Both high and low quality counterfeit goods are allegedly for sale in these shops showing intent to deceive consumers.

The enforcement authorities have conducted several raids against rogue merchants on the market, but stakeholders reported that most of the time the defendants are sentenced only to suspended sentences and the actions perceived not to be sufficient to reduce the level of counterfeiting on this market.

Ukraine

7th km market, Odessa

7th km market was reported by stakeholders for selling high volumes of counterfeit goods, mainly clothes, fashion accessories, perfumes and cosmetics. Products mainly come from China and Turkey and almost all the goods are allegedly counterfeit. It is one of the largest wholesale and retail market in Europe with 20,000 shops, pavilions, containers and warehouses and around 6,000 merchants.

Enforcement authorities reportedly do not perform raids and seizures on this market. The low sanctions and soft criminal responsibility for counterfeiters do not deter infringers. The market administrations are reportedly reluctant to cooperate with rightholders and to meet their requests.

The *Troyeshchyna Market* and *Khmelnitskiy Market* in Kiev and *Barabasova Market* in Kharkiv were also reported by stakeholders for the massive amount of counterfeit goods.

United Arab Emirates

Ajman China Mall

Ajman China Mall is a big distribution centre built together with warehouses, logistics and offices in the United Arab Emirates. With the occupied area of 280,000 square metres and the operating area of 100,000 square metres *Ajman China Mall* reportedly sells counterfeit goods, in particular bags, shoes, watches and electrical appliances, sunglasses, perfumes and toys. The market sells both at wholesaler and retailer level.

The enforcement authorities are reportedly not sufficiently active and do not conduct raids regularly in the *Ajman China Mall*.

Dragon Mart

Dragon Mart in the United Arab Emirates is allegedly the largest trading hub of counterfeit Chinese goods outside mainland China. It reportedly provides a gateway for the supply of counterfeit products mainly targeting Middle Eastern, North African and European markets. The 150,000 square metres retail complex allegedly offers both at wholesaler and retailer level a variety of high and low quality counterfeit goods and currently hosts over 3,950 outlets.

A wide variety of counterfeit products, including household and electrical appliances, stationery, office appliances, communication and acoustic equipment, lamps, building materials, furniture, toys, machinery, textiles, footwear, watches and fashion accessories are reportedly available on this market.

Stakeholders report that several raids are conducted each year by the enforcement authorities (in particular the Dubai Department of the Economic Development agents as well as the Dubai Police). Penalties include seizure of the products and fines, but the fines are perceived to be very low and not deterrent enough. Courts in the United Arab Emirates do not have authority to issue injunctions against landlords to prohibit the continuation of the IP infringements conducted by their tenants.

Jebel Ali Free Zone

Jebel Ali Free Zone in Dubai is a major regional distribution and logistics hub which serves as a model for other free trade zones in the region.

Stakeholders report that counterfeiters use the *Jebel Ali Free Zone* to manufacture, store and especially tranship allegedly counterfeit goods to various destinations, including the European Union. The counterfeit goods are transhipped through free trade zones in order to cleanse all the documents and to camouflage the original point of production and/or departure. *Jebel Ali Free Zone* is reportedly a distribution centre for counterfeit and pirated goods, "where shipments arrive in big volumes and are transhipped in smaller orders to their final destination points. Goods are often relabelled or repackaged in free zones, as in the *Jebel Ali Free Zone*. Consequently, in most cases it is difficult for customs officers to determine the country of origin, because of document cleansing and also because the actual process of counterfeiting may not take place in the same country as the production of a given good."[136]

Enforcement is perceived to be inefficient in *Jebel Ali Free Zone*, because until recently the only enforcement agency which had jurisdiction to take enforcement actions was the Dubai Police. The Dubai Department of Economic Development, which is reportedly the most active agency fighting against counterfeits, has no jurisdiction to enforce IP rights in free zones and only recently gained the ability to take actions in *Jebel Ali Free Zone* by signing a Memorandum of Understanding with the Dubai Police. Despite the MoU, sales of counterfeit products appear to remain rife in the *Jebel Ali Free Zone*.

The *Karama Shopping Complex* and *Gold Souq* in Dubai were also reported by stakeholders for the massive amount of counterfeit goods.

[136] See *footnote 30*

Vietnam

Saigon Square Plaza in Ho Chi Minh City

The *Saigon Square Plaza* is one of the well-known retail markets in Ho Chi Minh City, which offers a wide variety of allegedly counterfeit goods, in particular clothes, fashion accessories, shoes, phone accessories, cosmetics, beauty supplies, electronic appliances, jewellery and watches.

The enforcement authorities occasionally conduct raids in this plaza, but the high level of counterfeiting reportedly persists. The *Lucky Plaza* and *Ben Thanh Market* in Ho Chi Minh City were also reported by stakeholders for the massive amount of counterfeit goods.